CMRC
Crime Mapping Research Center

Crime Mapping and Data Confidentiality Roundtable July 8-9, 1999

Sponsored by: National Institute of Justice, Crime Mapping Research Center

Crime Mapping and Data Confidentiality Roundtable Overview Document

Background

In August of 1996, the concept of establishing a Crime Mapping Research Center within the National Institute of Justice emerged. During discussions among NIJ staff about the Center's plans and potential projects, it became evident that the mission of the Center could not be shaped without seeking counsel from experts in the field. Thus, NIJ convened a two-day Crime Mapping Strategic Planning Meeting to seek advice on the goals and direction of the Center. Several topics were raised at the initial planning meeting, one of which was the issue of data confidentiality in the development and dissemination of crime maps and geocoded crime data. Participants noted that criminal justice agencies are using GIS for a variety of applications: to allocate resources, to identify crime "hot spots," to aid in criminal investigations, and to support data-driven decision making processes. In addition, crime maps assist local law enforcement departments in enlisting public support for community policing strategies and efforts. Despite this widespread use of mapping in law enforcement, standards or guidelines outlining how crime maps and geocoded data should be generated and disseminated are not currently available.

Issues surrounding privacy and data sharing in crime mapping gained additional prominence at the Crime Mapping Research Center's second annual conference in 1998 and generated a profusion of postings on "Crimemap," the CMRC's listserv. Those who posted messages offered advice on the various types of crimes to map and at what level of aggregation. Listserv participants observed that the increased practice of sharing data across agencies and jurisdictional boundaries has elevated concerns about how much and what kinds of data should be shared. In addition, researchers are requesting greater access to geocoded crime data and prefer the data to be at the address level, which also raises important data sharing issues in terms of what data to share with researchers and with what restrictions. It was also noted that a partial solution to data sharing issues lies in various Internet and intranet firewalls and security measures, but these measures are often not accessible to the average law enforcement agency.

Based on the lively and provocative dialogue that has already taken place on this topic it has become clear that the CMRC should take a leadership role in this area. Therefore, we have convened this Crime Mapping and Data Confidentiality Roundtable to discuss these issues.

Purpose of the Roundtable

The Roundtable membership will include representatives from law enforcement, the research community, the legal profession, the GIS field, the media, victim advocacy, and the community. The purpose of the Roundtable is to generate discussion and initial guidance on issues of confidentiality, data sharing, and related security issues pertaining to crime mapping. A white paper compiled from transcripts of the Roundtable discussions will be developed and distributed to interested parties in the field.

The format and discussions of the Roundtable will be guided by the questions that appear below.

Where is the balance between the public's right to know and the victim's right to privacy? When a law enforcement agency posts a map of crime incidents on the Internet, it runs the risk of including too much or not enough data. For example, if a rape victim is identifiable, then his or her privacy has been violated. Yet if a rape is not posted and subsequently an individual falls victim to a rape, has the agency violated the public's "right to know"? That is, in not publishing the risk of rape in an area, is the agency failing to let would-be victims know they are at risk so they can take appropriate precautions?

Should professional standards or guidelines be developed for crime mapping as it pertains to privacy and freedom of information issues? If so, what should these standards look like and who should promote them? With the growing use of information technology in law enforcement, agencies are becoming increasingly concerned with their roles and responsibilities in creating and distributing crime maps and geocoded data. Individual agencies and analysts have experimented with "fuzzing" geocoded data and representing crime incidents and related data in various levels of aggregation, but no widely accepted standards or methods exist. Further, the Federal government has had limited success in issuing similar guidelines to local law enforcement in the past, raising the question of how local law enforcement might promote its own standards.

When information passes from one agency to another, who is liable or accountable for the inappropriate use of crime maps or the sharing of inaccurate geocoded data? What kind of statements should be made (i.e., disclaimers). A valid concern exists that disseminating crime maps to the public will revitalize informal redlining methods employed by some insurance and banking companies. Whereas a neighborhood identified as a high crime area could be targeted for various types of positive local interventions, it could also be flagged as undesirable, resulting in residential flight and ultimately causing more damage to an already problematic area. Further, the creation of crime maps or sharing of geocoded data that are inaccurate may result in false perceptions regarding the nature of a crime or public safety problem. Examples already exist of agencies publishing incorrect addresses of released sex offenders under Megan's Law, resulting in serious legal implications for such errors.

What is the appropriate model for partnerships between law enforcement agencies and researchers with regard to data sharing? Researchers are accustomed to signing agreements to ensure the confidentiality of individuals when analyzing survey data, but such agreements are not prevalent in the area of geocoded data. The field has yet to agree on what restrictions should be placed on researchers' use of data that will safeguard confidentiality while enabling researchers to experiment with rigorous analysis methods--methods that ultimately serve the entire criminal justice field.

What security measures are available for data sharing over Internet or intranet environments, and how can they be shared with local agencies? Setting up password protections, firewalls, and creating search and query options that block the display of particularly sensitive fields can be accomplished. However, police departments and officers have a healthy skepticism about the prospects of ensuring that intelligence information and other restricted data do not end up in the wrong hands. This calls for both public education on the reliability of such security measures as well as dissemination of specific methods for ensuring security.